15437-0589

1/14

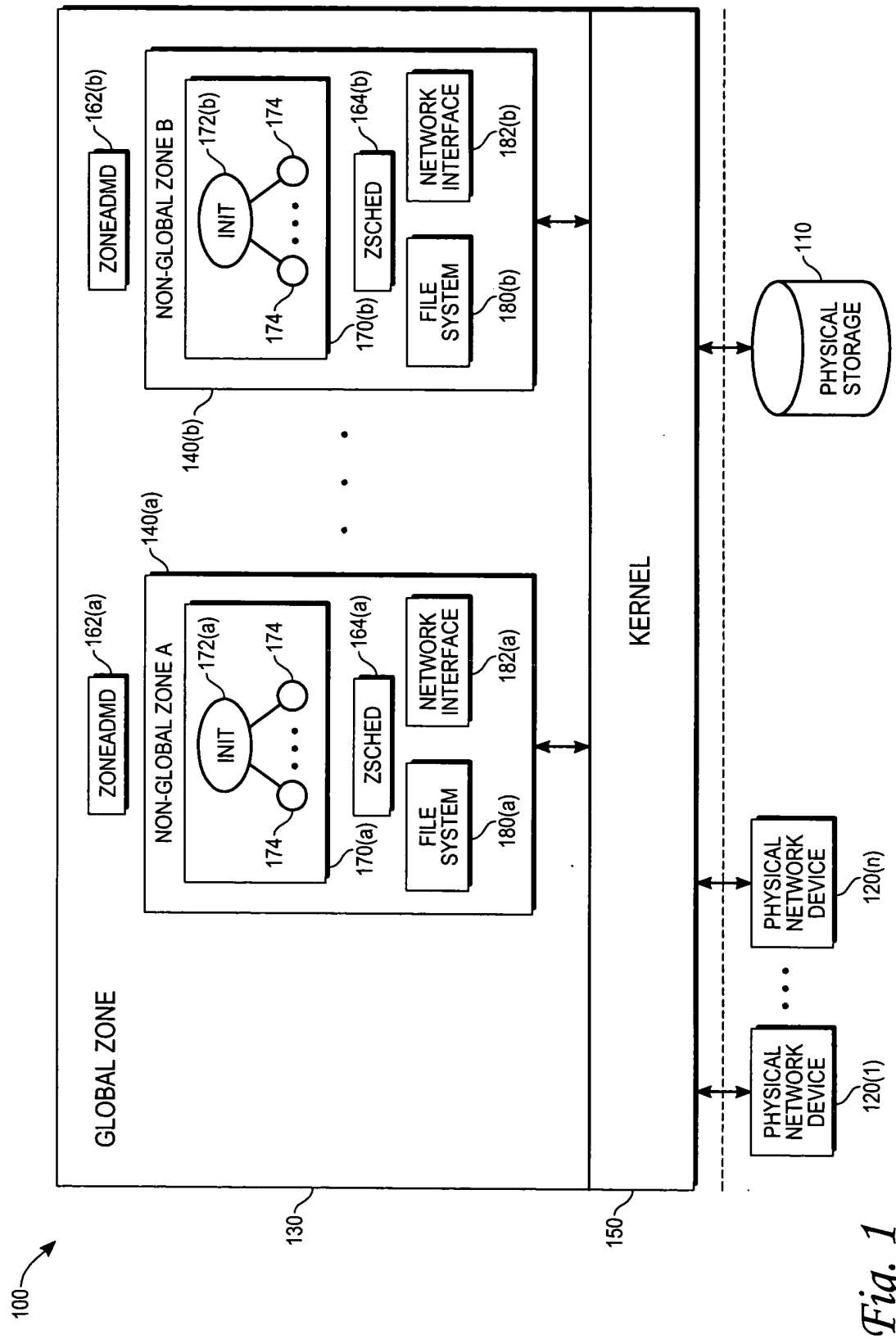

Fig. 1

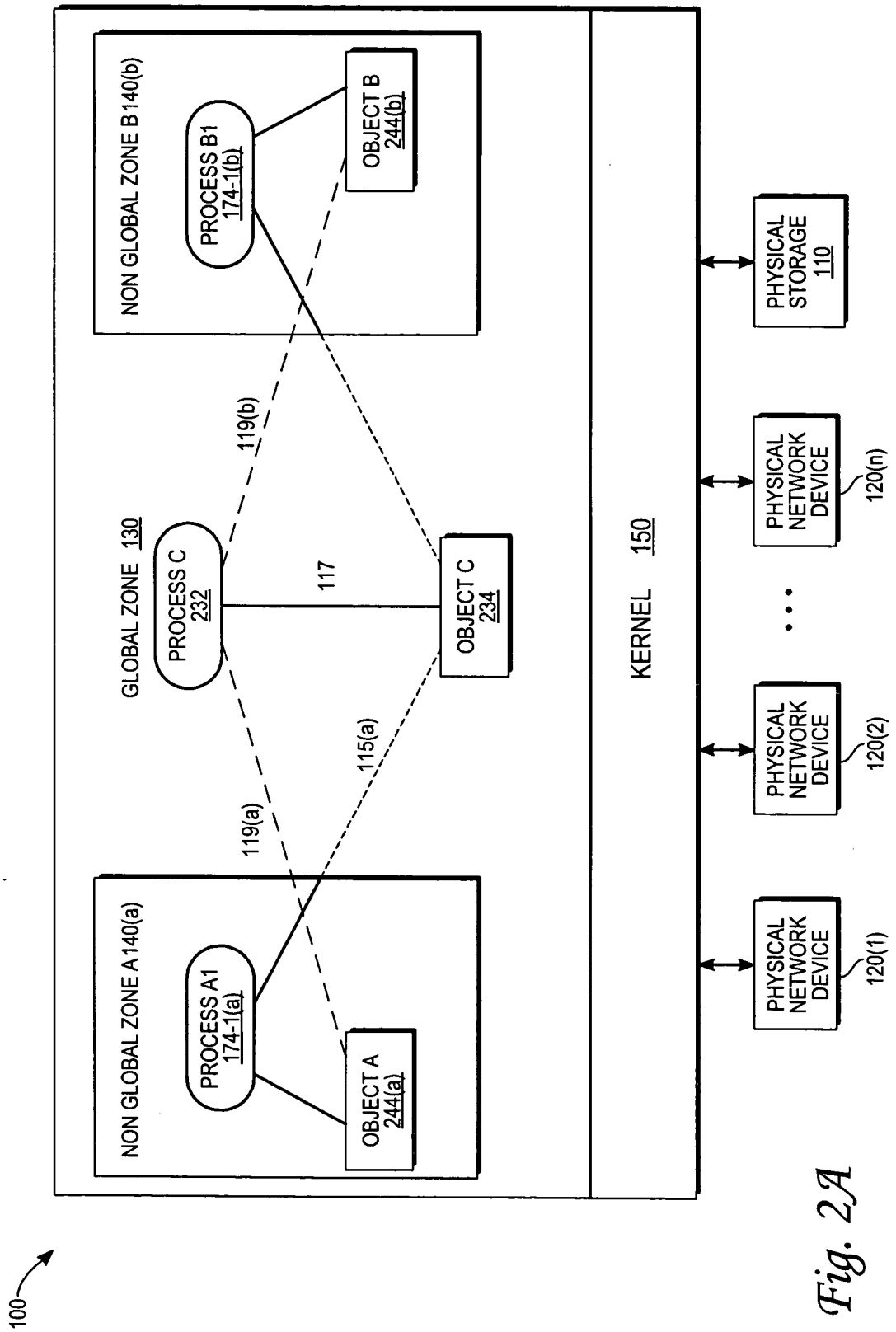
NON GLOBAL ZONE B 140(b)
PROCESS B1 174-1(b)
OBJECT B 244(b)
119(b)
GLOBAL ZONE 130
PROCESS C 232
117
OBJECT C 234
115(a)
119(a)
NON GLOBAL ZONE A 140(a)
PROCESS A1 174-1(a)
OBJECT A 244(a)
KERNEL 150
PHYSICAL STORAGE 110
PHYSICAL NETWORK DEVICE
120(n)
PHYSICAL NETWORK DEVICE
120(2)
PHYSICAL NETWORK DEVICE
120(1)
100

Fig. 2A

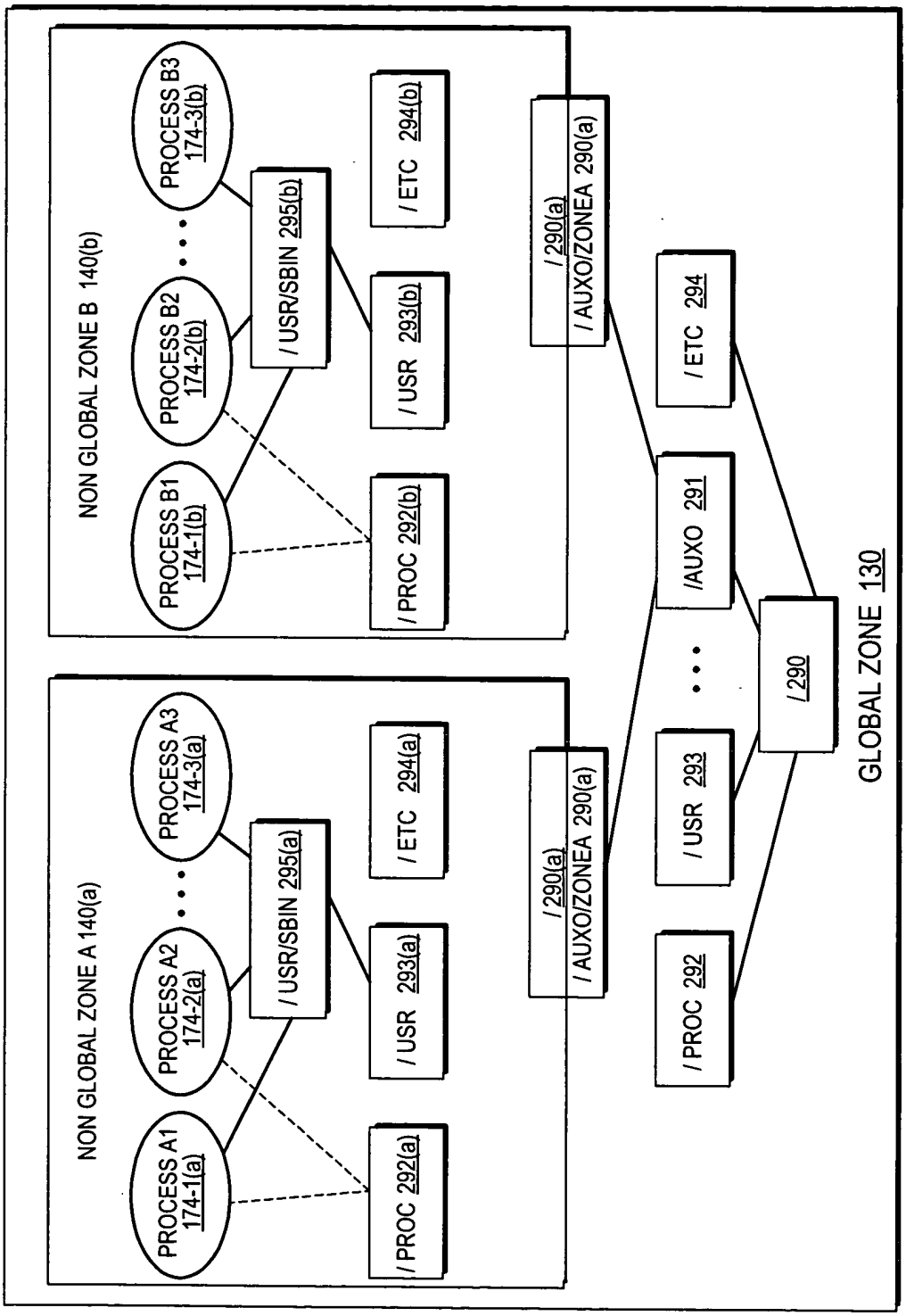
GLOBAL ZONE 130
NON GLOBAL ZONE A 140(a)
NON GLOBAL ZONE B 140(b)
PROCESS A1 174-1(a)
PROCESS A2 174-2(a)
PROCESS A3 174-3(a)
PROCESS B1 174-1(b)
PROCESS B2 174-2(b)
PROCESS B3 174-3(b)
/ PROC 292(a)
/ USR 293(a)
/ ETC 294(a)
/ USR/SBIN 295(a)
/ PROC 292(b)
/ USR 293(b)
/ ETC 294(b)
/ USR/SBIN 295(b)
/ 290(a) / AUXO/ZONEA 290(a)
/ 290(a) / AUXO/ZONEA 290(a)
/ PROC 292
/ USR 293
/ AUXO 291
/ ETC 294
/ 290
100

Fig. 2B

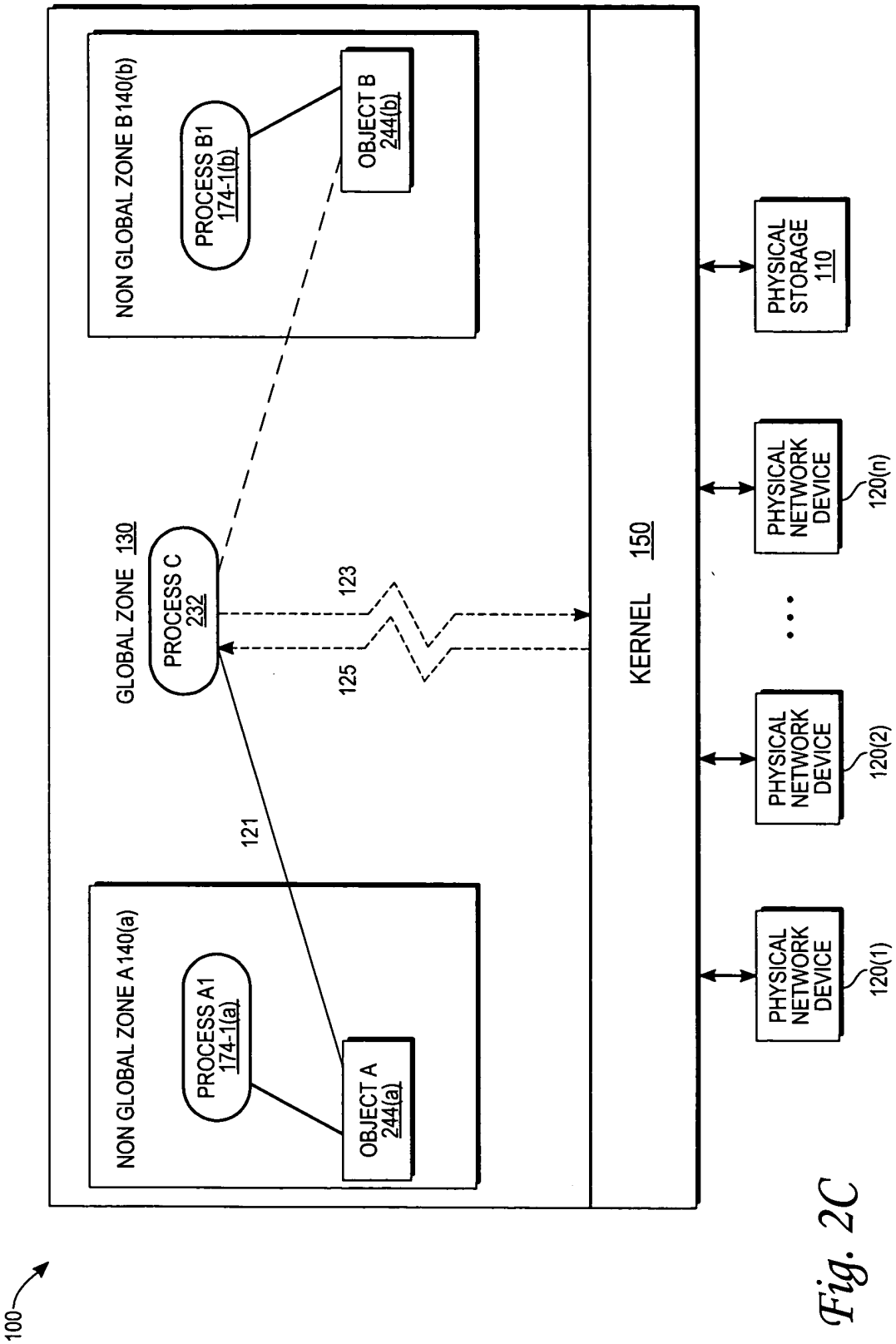
NON GLOBAL ZONE B 140(b)
PROCESS B1 174-1(b)
OBJECT B 244(b)
GLOBAL ZONE 130
PROCESS C 232
123
125
121
NON GLOBAL ZONE A 140(a)
PROCESS A1 174-1(a)
OBJECT A 244(a)
KERNEL 150
PHYSICAL STORAGE 110
PHYSICAL NETWORK DEVICE
120(n)
PHYSICAL NETWORK DEVICE
120(2)
PHYSICAL NETWORK DEVICE
120(1)
100

Fig. 2C

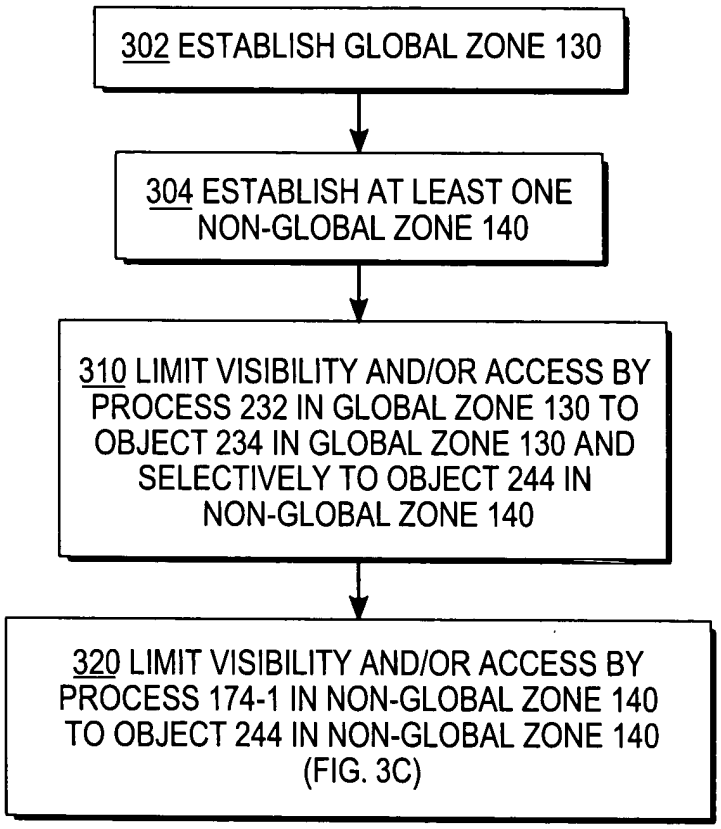
302 ESTABLISH GLOBAL ZONE 130
304 ESTABLISH AT LEAST ONE NON-GLOBAL ZONE 140
310 LIMIT VISIBILITY AND/OR ACCESS BY PROCESS 232 IN GLOBAL ZONE 130 TO OBJECT 234 IN GLOBAL ZONE 130 AND SELECTIVELY TO OBJECT 244 IN NON-GLOBAL ZONE 140
320 LIMIT VISIBILITY AND/OR ACCESS BY PROCESS 174-1 IN NON-GLOBAL ZONE 140 TO OBJECT 244 IN NON-GLOBAL ZONE 140 (FIG. 3C)

Fig. 3A

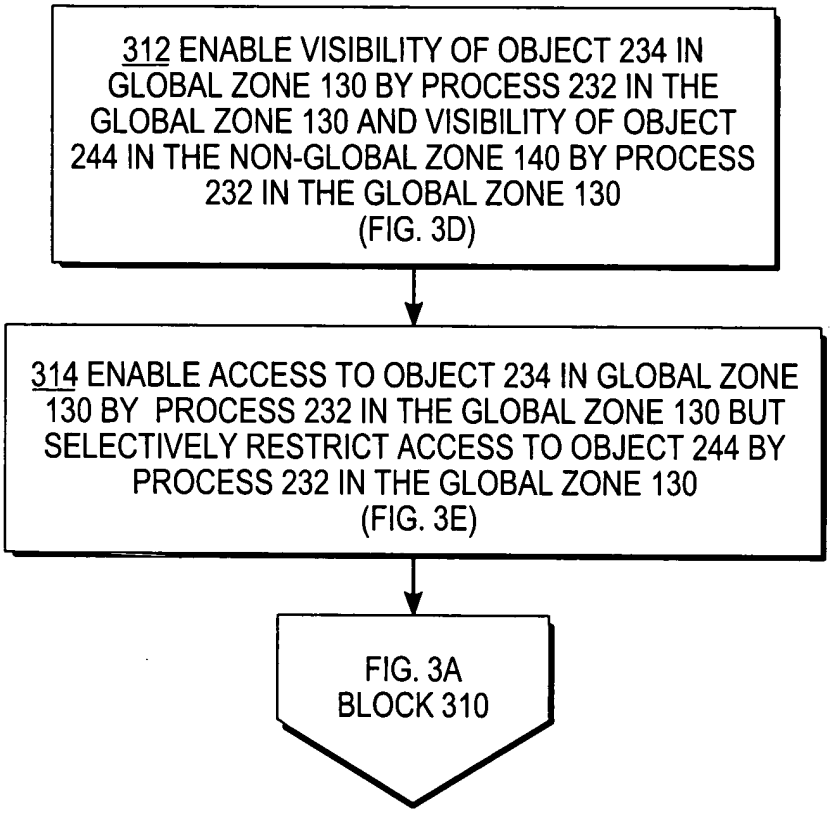
312 ENABLE VISIBILITY OF OBJECT 234 IN GLOBAL ZONE 130 BY PROCESS 232 IN THE GLOBAL ZONE 130 AND VISIBILITY OF OBJECT 244 IN THE NON-GLOBAL ZONE 140 BY PROCESS 232 IN THE GLOBAL ZONE 130
(FIG. 3D)
314 ENABLE ACCESS TO OBJECT 234 IN GLOBAL ZONE 130 BY PROCESS 232 IN THE GLOBAL ZONE 130 BUT SELECTIVELY RESTRICT ACCESS TO OBJECT 244 BY PROCESS 232 IN THE GLOBAL ZONE 130
(FIG. 3E)
FIG. 3A
BLOCK 310

Fig. 3B

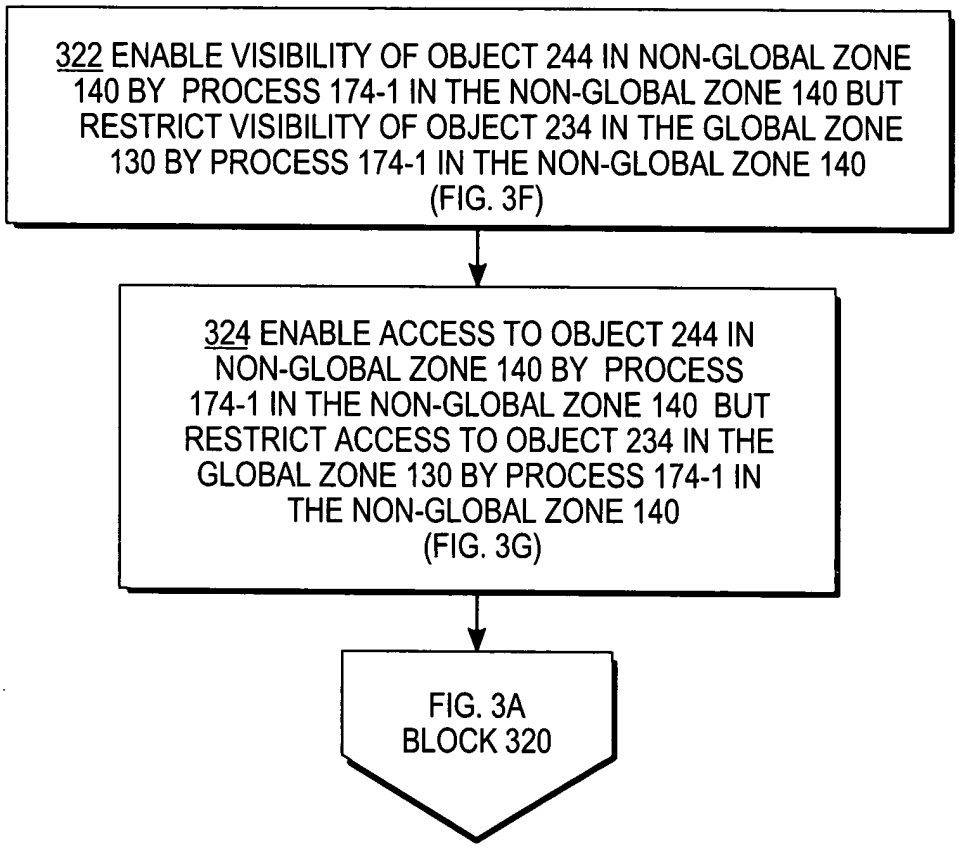
322 ENABLE VISIBILITY OF OBJECT 244 IN NON-GLOBAL ZONE 140 BY PROCESS 174-1 IN THE NON-GLOBAL ZONE 140 BUT RESTRICT VISIBILITY OF OBJECT 234 IN THE GLOBAL ZONE 130 BY PROCESS 174-1 IN THE NON-GLOBAL ZONE 140 (FIG. 3F)
324 ENABLE ACCESS TO OBJECT 244 IN NON-GLOBAL ZONE 140 BY PROCESS 174-1 IN THE NON-GLOBAL ZONE 140 BUT RESTRICT ACCESS TO OBJECT 234 IN THE GLOBAL ZONE 130 BY PROCESS 174-1 IN THE NON-GLOBAL ZONE 140 (FIG. 3G)
FIG. 3A BLOCK 320

Fig. 3C

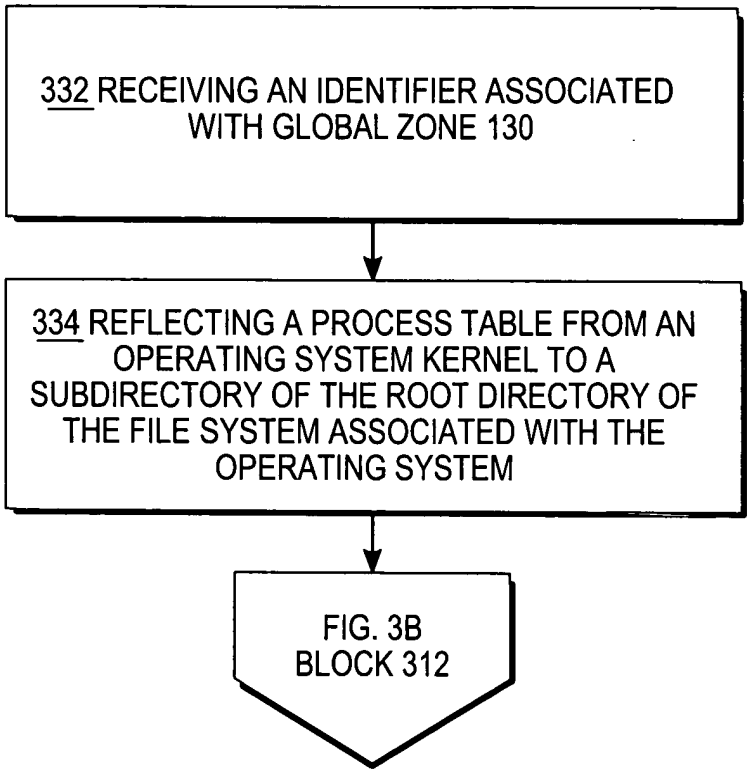
332 RECEIVING AN IDENTIFIER ASSOCIATED WITH GLOBAL ZONE 130
334 REFLECTING A PROCESS TABLE FROM AN OPERATING SYSTEM KERNEL TO A SUBDIRECTORY OF THE ROOT DIRECTORY OF THE FILE SYSTEM ASSOCIATED WITH THE OPERATING SYSTEM
FIG. 3B
BLOCK 312

Fig. 3D

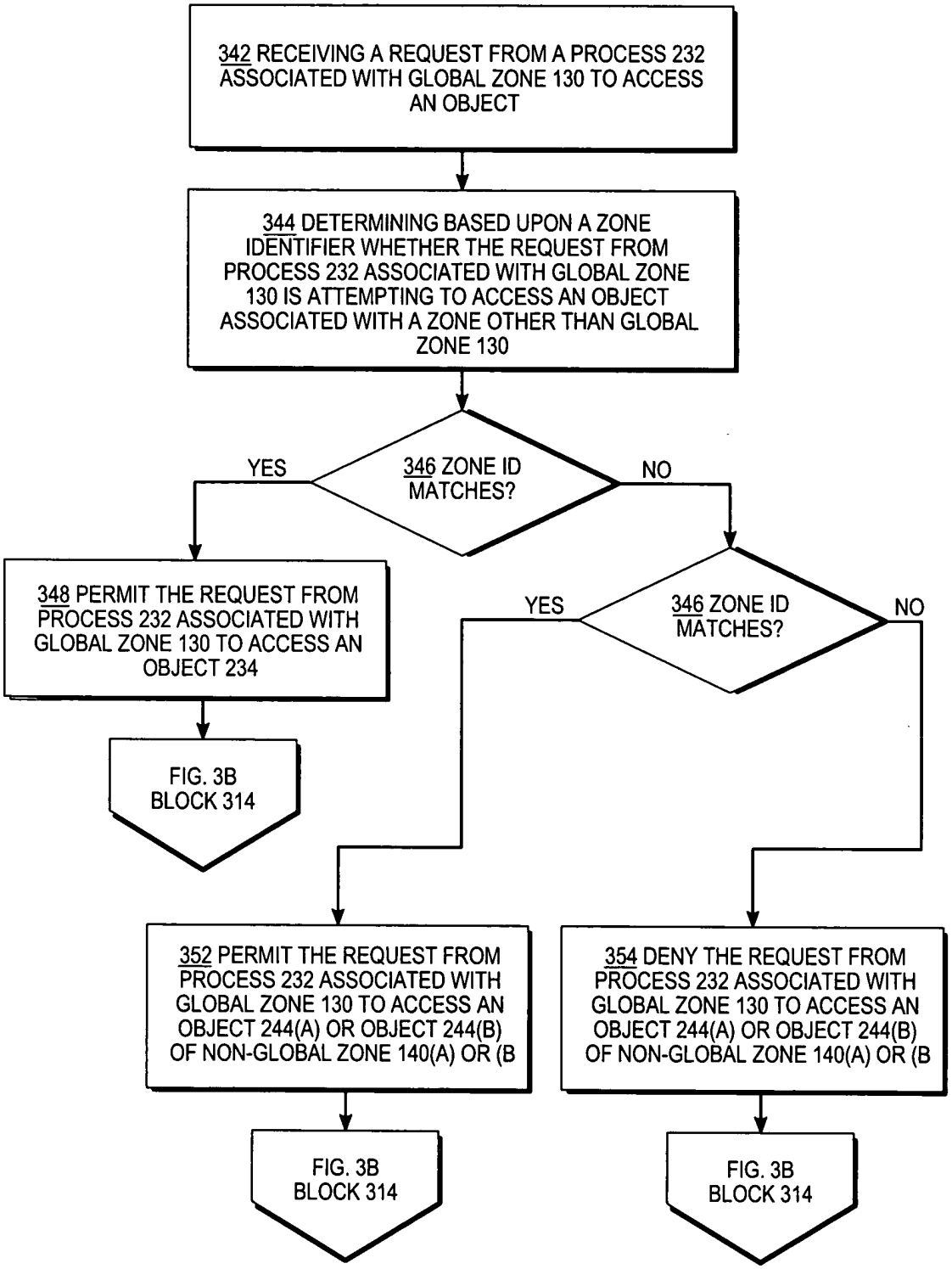
342 RECEIVING A REQUEST FROM A PROCESS 232 ASSOCIATED WITH GLOBAL ZONE 130 TO ACCESS AN OBJECT
344 DETERMINING BASED UPON A ZONE IDENTIFIER WHETHER THE REQUEST FROM PROCESS 232 ASSOCIATED WITH GLOBAL ZONE 130 IS ATTEMPTING TO ACCESS AN OBJECT ASSOCIATED WITH A ZONE OTHER THAN GLOBAL ZONE 130
346 ZONE ID MATCHES?
YES
NO
348 PERMIT THE REQUEST FROM PROCESS 232 ASSOCIATED WITH GLOBAL ZONE 130 TO ACCESS AN OBJECT 234
FIG. 3B BLOCK 314
346 ZONE ID MATCHES?
YES
NO
352 PERMIT THE REQUEST FROM PROCESS 232 ASSOCIATED WITH GLOBAL ZONE 130 TO ACCESS AN OBJECT 244(A) OR OBJECT 244(B) OF NON-GLOBAL ZONE 140(A) OR (B
354 DENY THE REQUEST FROM PROCESS 232 ASSOCIATED WITH GLOBAL ZONE 130 TO ACCESS AN OBJECT 244(A) OR OBJECT 244(B) OF NON-GLOBAL ZONE 140(A) OR (B
FIG. 3B BLOCK 314
FIG. 3B BLOCK 314

Fig. 3E

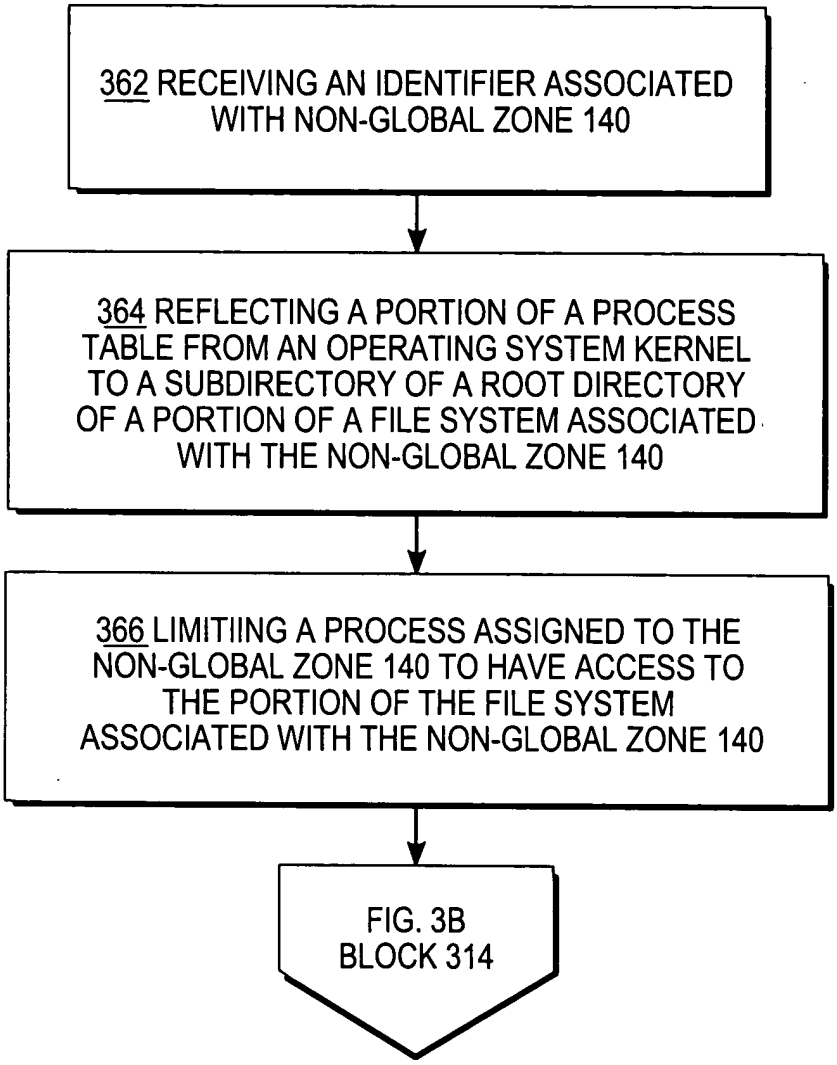
362 RECEIVING AN IDENTIFIER ASSOCIATED WITH NON-GLOBAL ZONE 140
364 REFLECTING A PORTION OF A PROCESS TABLE FROM AN OPERATING SYSTEM KERNEL TO A SUBDIRECTORY OF A ROOT DIRECTORY OF A PORTION OF A FILE SYSTEM ASSOCIATED WITH THE NON-GLOBAL ZONE 140
366 LIMITIING A PROCESS ASSIGNED TO THE NON-GLOBAL ZONE 140 TO HAVE ACCESS TO THE PORTION OF THE FILE SYSTEM ASSOCIATED WITH THE NON-GLOBAL ZONE 140
FIG. 3B
BLOCK 314

Fig. 3F

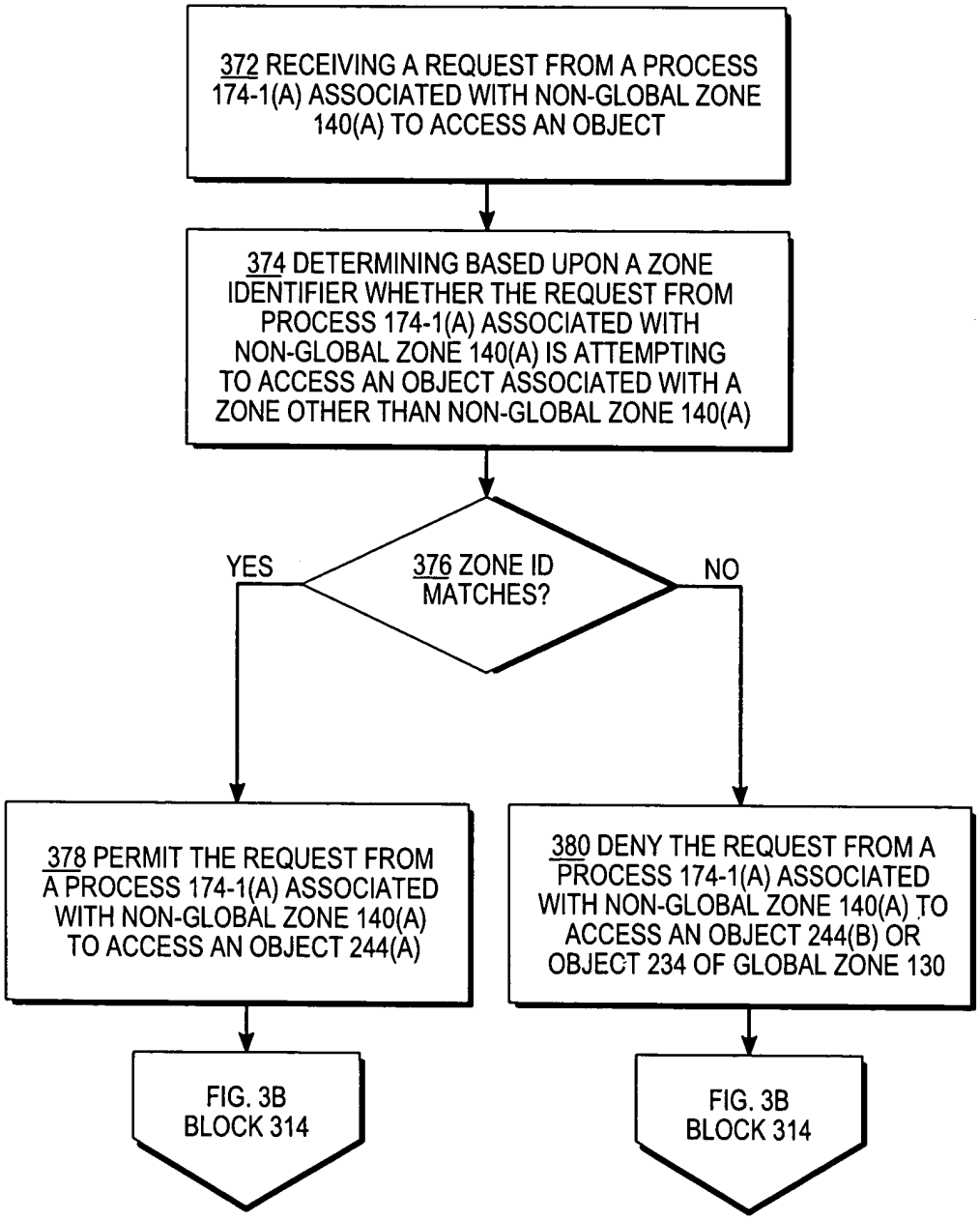
372 RECEIVING A REQUEST FROM A PROCESS 174-1(A) ASSOCIATED WITH NON-GLOBAL ZONE 140(A) TO ACCESS AN OBJECT
374 DETERMINING BASED UPON A ZONE IDENTIFIER WHETHER THE REQUEST FROM PROCESS 174-1(A) ASSOCIATED WITH NON-GLOBAL ZONE 140(A) IS ATTEMPTING TO ACCESS AN OBJECT ASSOCIATED WITH A ZONE OTHER THAN NON-GLOBAL ZONE 140(A)
376 ZONE ID MATCHES?
YES
NO
378 PERMIT THE REQUEST FROM A PROCESS 174-1(A) ASSOCIATED WITH NON-GLOBAL ZONE 140(A) TO ACCESS AN OBJECT 244(A)
380 DENY THE REQUEST FROM A PROCESS 174-1(A) ASSOCIATED WITH NON-GLOBAL ZONE 140(A) TO ACCESS AN OBJECT 244(B) OR OBJECT 234 OF GLOBAL ZONE 130
FIG. 3B BLOCK 314
FIG. 3B BLOCK 314

Fig. 3G

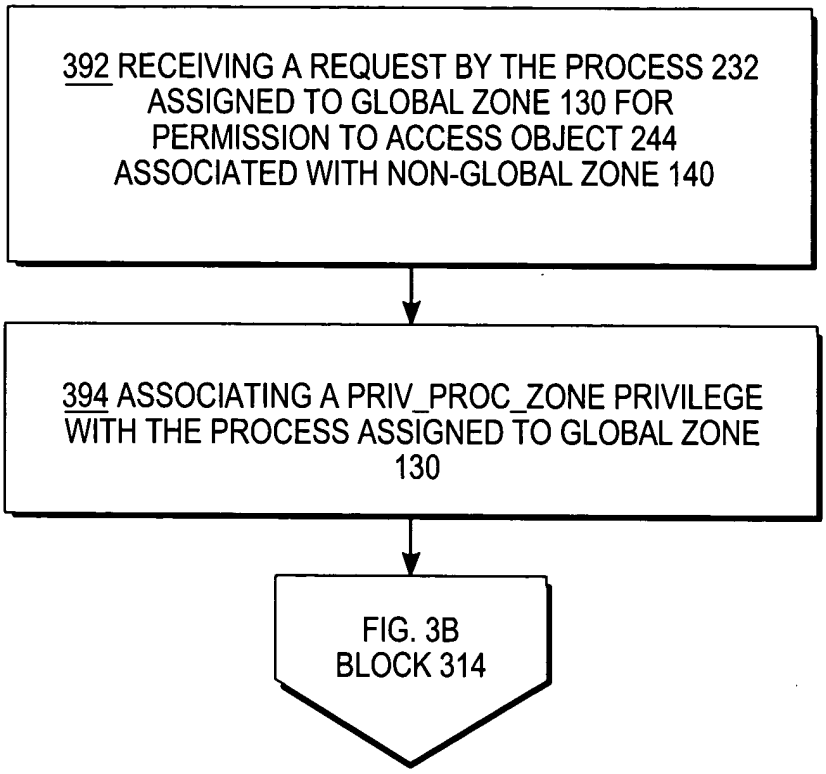
392 RECEIVING A REQUEST BY THE PROCESS 232 ASSIGNED TO GLOBAL ZONE 130 FOR PERMISSION TO ACCESS OBJECT 244 ASSOCIATED WITH NON-GLOBAL ZONE 140
394 ASSOCIATING A PRIV_PROC_ZONE PRIVILEGE WITH THE PROCESS ASSIGNED TO GLOBAL ZONE 130
FIG. 3B BLOCK 314

Fig. 3H

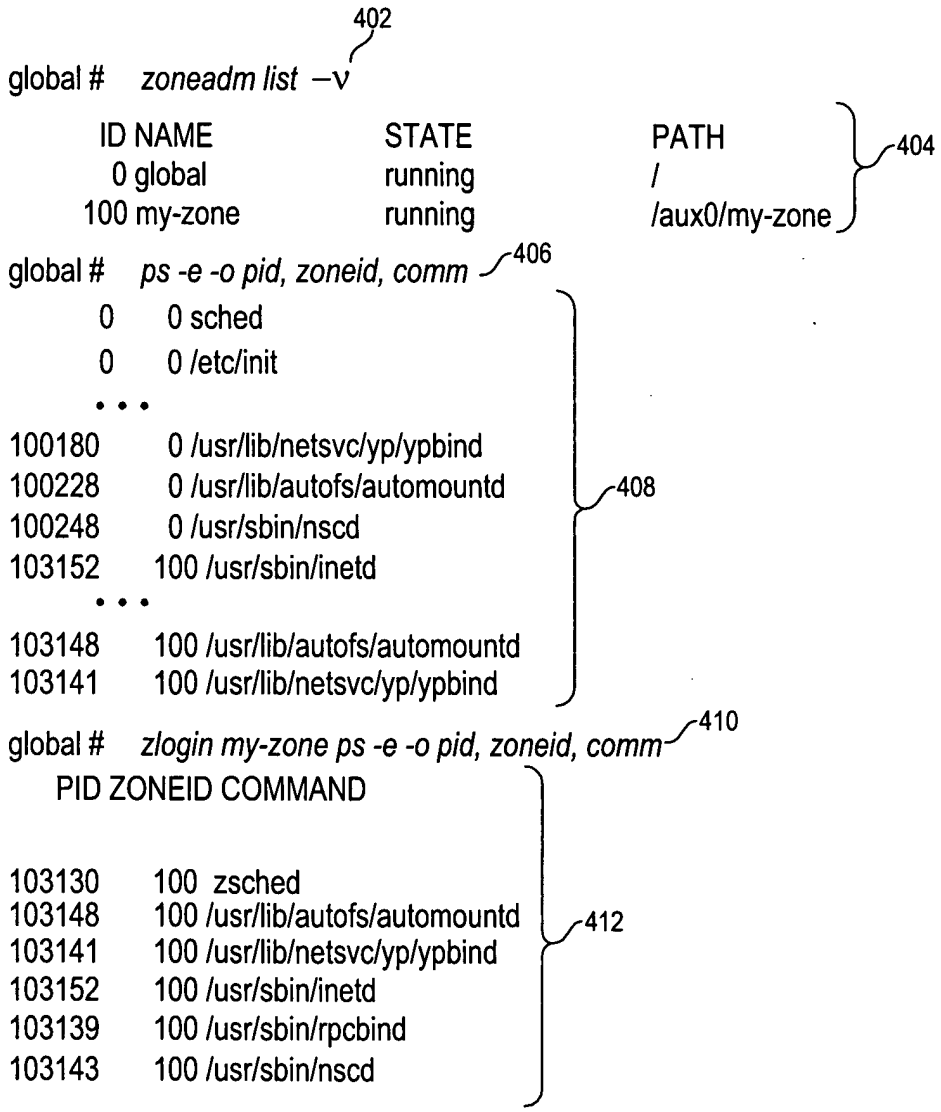
402
global # zoneadm list -v
ID NAME STATE PATH
0 global running /
100 my-zone running /aux0/my-zone
404
global # ps -e -o pid, zoneid, comm
406
0 0 sched
0 0 /etc/init
• • •
100180 0 /usr/lib/netsvc/yp/ypbind
100228 0 /usr/lib/autofs/automountd
100248 0 /usr/sbin/nscd
103152 100 /usr/sbin/inetd
• • •
103148 100 /usr/lib/autofs/automountd
103141 100 /usr/lib/netsvc/yp/ypbind
408
global # zlogin my-zone ps -e -o pid, zoneid, comm
410
PID ZONEID COMMAND
103130 100 zsched
103148 100 /usr/lib/autofs/automountd
103141 100 /usr/lib/netsvc/yp/ypbind
103152 100 /usr/sbin/inetd
103139 100 /usr/sbin/rpcbind
103143 100 /usr/sbin/nscd
412

Fig. 4

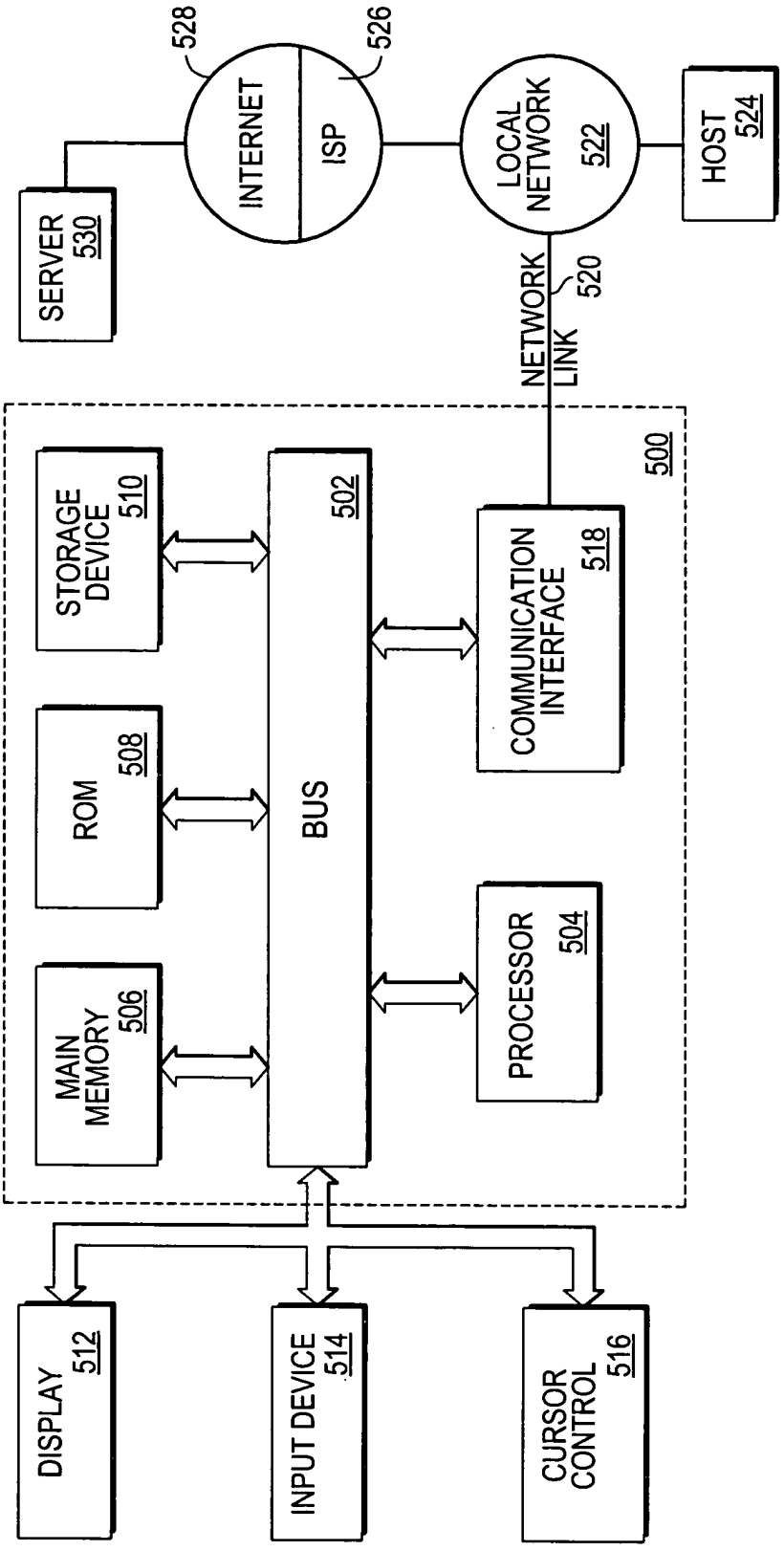
528
526
INTERNET
ISP
LOCAL NETWORK 522
HOST 524
SERVER 530
NETWORK LINK 520
500
STORAGE DEVICE 510
502
COMMUNICATION INTERFACE 518
ROM 508
BUS
PROCESSOR 504
MAIN MEMORY 506
DISPLAY 512
INPUT DEVICE 514
CURSOR CONTROL 516

Fig. 5